National Infrastructure Protection Center CyberNotes

Issue #25-99 *December 8, 1999*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between November 19, and December 3, 1999. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold. New information contained in the update will appear as red and/or italic text.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
American Power Conversions (APC), Inc.[1]	PowerChute Plus 5.1 for Windows NT	A Denial of Service vulnerability exists which enables remote malicious attackers to connect to ports, 6667 or 6668, crashing the system.	Upgrade to version 5.2, which should be out around the end of December. Version 5.2Beta is available at: http://www.apcc.com/tools/download/sw_kit.cfm?sku=sdw27	PowerChute Plus Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Arcane Software[2]	Vermillion FTP Daemon 1.23	Buffer overflow exist in Vermillion FTP Daemon (VFTPD) which can cause a denial-of-service condition and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Remote Denial of Service Vulnerability	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[1] Bugtraq, November 24, 1999.
[2] UssrLabs, November 22, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
BisonWare[3]	BisonWare FTP Server 3.5	A local/remote Denial of Service vulnerability exists in BisonWare FTP Server when a long user name, 2000 characters is entered.	No workaround or patch available at time of publishing.	Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Cabletron[4]	SmartSwitch Router 8000 Firmware v2.x	A Denial of Service vulnerability exists in the ARP handling mechanism of the SmartSwitch Router (SSR).	Upgrade your SSR firmware to version 3.x located at: http://www.cabletron.com/download/download.cgi?lib-ssr	SmartSwitch Router Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites.
Caldera[5]	Pine prior to 4.2.1	It is possible to cause Pine to execute shell commands upon visiting a URL.	Upgrade to the latest package at: ftp://ftp.calderasystems.com/pub/OpenLinux/updates/2.3/current/RPMS	URL Vulnerability	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit has been published.
Deerfield.com[6]	MDaemon Server 2.8.5.0; Mdaemon 2.7 Japanese	Multiple remote Denial of Service vulnerabilities exist due to improper bounds checking which can cause the system to crash and possibly execute arbitrary code. The affected remote services are: WorldClient: Port 2000 and WebConfig: Port 2002	Patch for Mdaemon/WorldClient standard can be found at: http://www.altm.com/Downloads/incoming/md285fix.zip A hotfix for WorldClient Pro is available at: http://www.worldclient.com/helpdesk/hotfix.cgm	Denial of Service Vulnerability	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Deerfield.com[7]	Serv-U FTP Server v2.5a	A buffer overflow vulnerability exists which causes the FTP Server to crash and execute arbitrary code when a malicious user executes the SITE command.	No workaround or patch available at time of publishing.	Remote Buffer Overflow Vulnerability	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit has been published.

[3] UssrLabs, November 24, 1999.
[4] Bindview Security Advisory, November 24, 1999.
[5] Caldera Systems, Inc. Security Advisory, CSSA-1999-036.0, November 19, 1999.
[6] UssrLabs, November 24, 1999.
[7] UssrLabs, November 2, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
FreeBSD[8]	FreeBSD 3.3	Vulnerabilities exist in seyon, xmindpath, angb and gdc, which will allow certain users to gain root privileges and overwrite system files.	No workaround or patch available at time of publishing.	Multiple FreeBSD Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Hewlett-Packard[9]	HP9000 Series 800 S/X/V Class Servers	A vulnerability exists which allows remote users to access the S/X/V/ Class console via the Service Support Processor (SSP) Teststation.	Install the applicable patch on the SSP/Teststations, or install Teststation Version 5.1.2 software on any V22x0 product, or Teststation Version 1.1.2 on any V2500 product. The patch package can be retrieved from the Electronic Support Center ftp site: ftp://us-ffs.external.hp.com/firmware_patches/hp_cpu/PF_CSXV1007	V Class Teststation Security Vulnerability	Medium	Bug discussed in newsgroups and websites.
Hewlett-Packard[10]	JetDirect J3111A	The webserver for remote printer administration contains a buffer overflow vulnerability in the code that handles incoming URLs, possibly making the printer execute arbitrary code.	No workaround or patch available at time of publishing.	JetDirect Webserver URL Denial of Service Vulnerability	Medium/ Low	Bug discussed in newsgroups and websites. Exploit has been published.
InterSoft[11]	NetTerm FTP Daemon 4.2.1, 4.2.2, 4.2.1	A number of security vulnerabilities exist which are caused by the default configuration and inadequate buffer checking code.	No workaround or patch available at time of publishing.	NetTerm Security Vulnerabilities	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Linux[12]	All Linux systems using the syslog daemon	Vulnerability exists in the current syslogd daemon, which allows any user on the local host to mount a Denial of Service attack that effectively stops all logging.	Upgrade to the latest version of syslogd (depending on your Linux distribution).	LINUX syslog Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[13]	Internet Explorer 5	A vulnerability exists which allows a malicious user to provide proxy settings to web clients in another network, effectively performing URL hijacking.	Patch available at: http://www.microsoft.com/windows/ie/download/all.htm?bShowPage	WPAD Spoofing Vulnerability	**High**	Bug discussed in newsgroups and websites.

[8] Bugtraq, November 30, 1999.
[9] Hewlett-Packard Company Security Advisory, #00105, November 24, 1999.
[10] SecurityFocus, November 19, 999.
[11] Bugtraq, November 22, 1999.
[12] Securiteam, November 22, 1999.
[13] Microsoft Security Bulletin, MS99-054, December 2, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[14]	Internet Explorer 5.0	Frame spoofing is possible under the default security settings. This vulnerability allows misleading the user into thinking he/she is browsing a trusted site, while in fact they may be browsing a hostile site, which might be stealing information.	No workaround or patch available at time of publishing. Unofficial solution: Set "Navigate sub-frames across different domains" option to disable.	IE5 Frame Spoofing Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[15]	Internet Explorer 5.0 for Windows NT 4.0, 2000, 98, 95	A vulnerability exists which exposes the user's local files when processing HTTP redirects within the Extensible Markup Language (XML) objects.	No workaround or patch available at time of publishing. Unofficial workaround: Disable active scripting	IE5 XML HTTP Redirect Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the Press.
Microsoft[16]	Internet Explorer 5 for Windows NT 4.0	IE5 Task Scheduler contains a vulnerability in an optional component which could allow a malicious user to gain additional privileges on a Windows NT machine allowing him or her to create or change files.	The vulnerability is eliminated by IE 5.01, which is available at: http://www.microsoft.com/msdownload/iebuild/ie501_win32/en/ie501_win32.htm	IE5 Task Scheduler Privilege Elevation Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[17]	SQL Server 7.0	A Denial of Service vulnerability exists in the MS SQL Server, which causes it to crash silently when a TCP packet that contains more than two NULLS as the TCP data is sent.	No workaround or patch available at time of publishing.	NULL Data Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft[18]	Windows 95, 98	Security vulnerability exists which lets a local user gain authentication information of previous users of that particular system.	Patch available at: Windows 95 http://download.microsoft.com/download/win95/update/168115/w95/en-us/168115us.exe Windows 98 http://download.mcirosoft.com/download/win98/update/168115/w98/en-us/168115us.exe	Legacy Credential Caching Vulnerability	Medium	Bug discussed in newsgroups and websites.

[14] Bugtraq, November 30, 1999.
[15] SecurityFocus, November 22, 1999.
[16] Microsoft Security Bulletin, MS99-051, November 29, 1999.
[17] SecurityFocus, November 23, 1999.
[18] Microsoft Security Bulletin, MS99-052, November 29, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft Windows 98/NT[19] ***Update to WordPad vulnerability[20]***	**WordPad**	**Win98/NT4 Riched20.dll (which WordPad uses) has a buffer overflow problem with ".RTF-files, which could result in executing arbitrary code. The code can be put into an .RTF file and mailed to the victim.** ***The vulnerability doesn't appear to offer a means of executing arbitrary code, so the risk is limited to that of a minor nuisance.***	**No workaround or patch available at time of publishing.**	**WordPad Buffer Overflow Vulnerability**	**Medium /High** ***Low***	**Bug discussed in newsgroups and websites. Exploit script has been published.** ***New script that exploits this vulnerability has been published.***
Netscape[21]	Netscape Communi-cator 4.6, 4.7	Vulnerability exists which causes Netscape to crash when a URL containing long variables is entered. When this happen Netscape Navigator crashes and executes the arbitrary buffer passed by the URL.	No workaround or patch available at time of publishing.	URL Variable Overflow Vulnerability	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit has been published.
Netscape[22]	Netscape Enterprise; FastTrack	A buffer overflow vulnerability exists in the HTTP Basic Authentication portion of the server that can be used to execute code on the machine as SYSTEM in Windows NT or as root or nobody in Unix, without requiring authentication. This vulnerability affects all supported platforms of Enterprise and FastTrack web servers.	No workaround or patch available at time of publishing.	Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. .
Nosque Workshop[23]	ZetaMail 2.0, 2.1	The ZetaMail Mail Server will crash if a username and password is entered that is 3500 characters in length.	Upgrade to the latest version located at: http://www.web-net.com/supermail/MsgCoreNT_210.zip or http://www.web-net.com/supermail/MsgCore95_211.zip	ZetaMail Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Oracle[24]	Oracle Web Listener	Security vulnerability exists in the Oracle bundle that allows remote malicious users to gain access to restricted files.	No workaround or patch available at time of publishing.	Oracle Web Listener Permission Vulnerability	Medium	Bug discussed in newsgroups and websites.

[19] Bugtraq, November 18, 1999.
[20] SecurityFocus, November 22, 1999.
[21] Bugtraq, November 24, 1999.
[22] Internet Security Systems (ISS) Security Advisory, December 1, 1999.
[23] UssrLabs, November 18, 1999.
[24] Securiteam, November 27, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
ProFTPD[25]	ProFTPD 1.2pre1	Compiling the mod_sqlpw module makes it possible for local users to view the passwords of users who have connected to the ftp server.	No workaround or patch available at time of publishing.	ProFTPD Cleartext Password Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Qualcomm[26]	Qpopper 3.0b, 3.02b	A buffer overflow vulnerability exists that can be exploited remotely and lead to a root compromise. The overflow occurs in the AUTH parsing function	This is fixed in qpopper3.0b22, which is now available.	Qpopper Remote Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
RedHat[27] ***Update to fix functionality vulnerabilities*** [28]	**Linux 6.1**	**A vulnerability exists in login if you are using csh/tcsh, which makes it possible to execute arbitrary commands. The problem has to do with the Initscripts for these shells that run when the user logs in and a /tmp race condition that they are vulnerable to.** ***One security vulnerability and several functionality vulnerabilities have been fixed in a new release of initscripts for Intel platforms only.***	**Upgrade your Initscripts package:** **ftp://updates.redhat.com/6.1/i386/initscripts-4.63-1.8386.rpm** ***Upgrade to the fixed packages located at:*** ***Intel:*** ftp://updates.redhat.com/6.1/i386/initscripts-4.67-1.i386.rpm ***Sparc:*** ftp://updates.redhat.com/6.1/sparc/initscripts-4.67-1.sparc.rpm ***Intel:*** ftp://updates.redhat.com/6.1/SRPMS/initscripts-4.67-1.src.rpm	**Tmp Race Vulnerability**	**High**	**Bug discussed in newsgroups and websites.**
SCO[29]	UnixWare 2.1.3; 7.0.0 through 7.1.1	Several security vulnerabilities have been found in the "su" program along with the iaf library.	SCO is providing an interim patch to address this issue in the form of a System Security Enhancement (SSE) package. You can download the SEE package at: Cover Letter: ftp://ftp.sco.COM/SSE/sse039.ltr New Binaries: ftp://ftp.sco.COM/SSE/sse039.tar.z	SCO Su Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.

[25] SecurityFocus, November 19, 1999.
[26] Bugtraq, November 30, 1999.
[27] RedHat, Inc. Security Advisory, RHSA-1999:052-01, November 8, 1999.
[28] RedHat, Inc. Security Advisory, RHSA-1999:052-02, November 23, 1999.
[29] SCO Security Bulletin, 99.19, November 28, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Sun Microsystems[30]	NetBeans (recently renamed to Forte') Java IDE	A security vulnerability exists which opens the computer to a remote compromise; this is due to a programming error, which allows anyone from a remote computer to connect to the locally open HTTP server which is installed by NetBeans.	No workaround or patch available at time of publishing. Unofficial Solution (work around): 1) Set the HTTP Server "Enable" setting to False in Project settings. or 2) Remove the HTTP Server module in Global settings.	NetBeans/Forte Java IDE HTTP Vulnerability	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Microsystems[31]	Solaris 7	Security vulnerability exists in the 'kcms_configure', which can be used to gain root access.	No workaround or patch available at time of publishing.	Kcms_ configure Buffer Overflow Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Sun Microsystems[32]	Solaris 7 Mailer Programs	The mailer programs (mailtool and dtmail) and mail message print filter (dtmailpr) contain a buffer overflow vulnerability which gives any user the capability to read/write other user's mail files.	No workaround or patch available at time of publishing.	Mail Programs Buffer Overflow Vulnerabilities	Medium	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Sun Microsystems[33]	Solaris 7.0, 7.0_x86	A Denial of Service vulnerability exists in rpc.ttdbserver. A NULL pointer being dereferenced when rpc finding is called with garbage causes this problem.	Install patch id# 107893-02 located at: ftp://sunsolve.Sun.COM/pub/patches/Solaris.PatchReport	Rpc.ttdbserver Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. .
Symantec[34]	Mail-Gear v.1.0	The Mail-Gear Web Interface Server is vulnerability to Directory Traversal. A malicious user can read any file on the local drive, including files outside the bounding HTML directory.	Upgrade to Mail-Gear 1.1	Directory Traversal Vulnerability	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Tektronix[35] ***Printer update.[36]***	**PhaserLink 740**	**A vulnerability exists which shows the administrator password to anyone without authentication.** ***The Phaser Color printer 780 and 840 also contain the same vulnerability.***	**No workaround or patch available alt time of publishing. Unofficial workaround: Block Port 80 access to this printer via a router or firewall, or disable the PhaserLink webserver on the printer.**	**PhaserLink Webserver Vulnerability**	**Low**	**Bug discussed in newsgroups and websites. Exploit has been published.**

[30] Bugtraq, November 24, 1999.
[31] Securiteam, November 30, 1999.
[32] Securiteam, December 1, 1999.
[33] SecurityFocus, November 19, 1999.
[34] Securiteam, November 30, 1999.
[35] Bugtraq, November 16, 1999.
[36] Securiteam, November 23, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
WU-FTPD Development Group[37] ***Improved exploit code released.***[38]	**All platforms using: wu-ftpd-2.4.2-beta-18-vr4 through beta-18-vr15; wu-ftpd-2.4.2-vr16, vr17; wu-ftpd-2.5.0; BeroFTPD, all present versions; other derivatives of wu-ftpd may be effected**	**A vulnerability exists in wu-ftpd that may allow local and remote users to gain root privileges.**	**The Wu-FTPD Development Group has made the following patch available for wu-ftpd 2.5.0: ftp://ftp.wu-ftpd.org/pub/wu-ftpd/quickfixes/apply_to_2.5.0 Users of BeroFTPD 1.3.4 can apply the same patch.**	**Wu-FTPD Buffer Overflow Vulnerability**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.** ***Improved exploit code has been released, the new code includes well-known offsets and a good method on how to find new ones.***

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between November 19, and December 2, 1999, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 58 scripts, programs, and net-news messages containing holes or exploits were identified.

[37] SecurityFocus, August 31, 1999.
[38] Securiteam, November 23, 1999.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
December 2, 1999	**Ex_kcms_configuresp.c**	**Exploit script for the kcms_configure vulnerability in Solaris.**	
December 2, 1999	Pandora_linux-v4.0_b2.1.tgz	Pandora v4 Beta netware attack tool for Linux.	
December 2, 1999	Sambar.remote.dos.txt	Sambar Web Server Denial of Service vulnerability technique.	
December 2, 1999	Unixware7.uidadmin.txt	Exploit script for UnixWare 7.1 uidadmin vulnerability, which will allow any user to gain root privileges.	
December 1, 1999	**1991-exploits.tgz**	**New exploits for November 1999.**	
December 1, 1999	**Arb-dos.tar.gz**	**Three perl scripts that exploit recent Windows application Denial of Service vulnerabilities in Avirt Mail Server, Byte Fusion Telnet, and Vermillion FTP Daemon.**	
December 1, 1999	**Ex_dtmailpr.c**	**Solaris7 dtmailpr exploit script.**	
December 1, 1999	**Freebsd.seyon.txt**	**Exploit script for the FreeBSD seyon vulnerability.**	
December 1, 1999	**Gdcx.c**	**Gdc exploit script for gated-3.5.11 included in FreeBSD 3.3.**	
December 1, 1999	**Ie50.frame-spoofing.txt**	**Exploit script for the frame spoofing vulnerability in Internet Explorer 5.**	
December 1, 1999	Q3mash.c	Qpopper 3.0b remote exploit script for x86 Linux.	
December 1, 1999	Qpop-sk8.c	Qpopper 3.0b remote root exploit script for BSDI 3.0/4.01, FreeBSD 2.2.8/3.3 and Linux.	
December 1, 1999	**Xmindx.c**	**Exploit script for the xmindpath vulnerability in FreeBSD 3.3**	
November 30, 1999	Apsend.tar.gz	Denial of Service exploit script for Windows 95/98/NT.	
November 30, 1999	Netscape.4.x.java.txt	Exploit for Netscape Communicator 4.x, which allows JavaScript code in one Netscape window to read data from another browser window.	
November 30, 1999	Q3combo-public.c	Exploit script that works on BSD and Linux for the qpopper vulnerability.	
November 29, 1999	**Ex_mailtool.c**	**Solaris7 mailtool exploit script, which allows any local user to read/write any user's mailbox.**	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
November 29, 1999	Exploit.txt	A tutorial on how to write shellcode and exploits and how buffer overflows work in general.	
November 29, 1999	Fwg.c	A program that mimics the functionality of WinGate, except it logs the entire session.	
November 29, 1999	Mailgear-1.0.txt	Symantec Mail-Gear 1.0 web interface server directory transversal vulnerability script.	
November 29, 1999	**MDAC-scan.pl**	**Msadc scanner written in perl.**	
November 29, 1999	**Msadcscan-lux.c**	**Final release of msadc scanner.**	
November 29, 1999	**Nmap-2.3BETA6-vulnmap.tgz**	**Vulnerability scanning modifications to Nmap v2.3BETA6.**	
November 29, 1999	NSS_253.tar.gz	Perl script, which checks for 190 remote vulnerabilities.	
November 29, 1999	Portfwd-0.0.tar.gz	Portfwd forwards incoming TCP connections and/or UDP packets to remote hosts. Multiple forwarders can be specified in a flexible configuration file format.	
November 29, 1999	RA-AnonEmail.zip	An anonymous e-mail program that can send e-mail to anyone and you, the user, can make it look like it came from any address.	
November 29, 1999	RA-Cache.zip	A tool that finds cached passwords on your computer.	
November 29, 1999	RA-Portscan.zip	A Windows-based portscanner that scans a remote computer and looks for open ports.	
November 29, 1999	Scanner.zip	A powerful connect-based TCP port scanner, pinger and hostname resolver.	
November 29, 1999	Smailx.sh	Remote root exploit script for Smail-3.2.	
November 29, 1999	Ss-1.3.tgz	A combination of esniff.c and tcpdump. This allows network sniffing on busy networks with much fewer packet drops.	
November 29, 1999	Wpc-0_1b.tar.gz	A simple application that tries to guess usernames and passwords for password protected web pages.	
November 26, 1999	Unixware-xlock.txt	Exploit script for the buffer overflow vulnerability in UnixWare 7'x xlock.	
November 24, 1999	Ex_bbc.c	Script which exploits a bounds checking error in /usr/jp/bin/mh/bbc which was distributed with the mh-6.8.c package.	
November 24, 1999	Ex_inc.c	Script which exploits a bounds checking error in /usr/jp/bin/mg/inc which was distributed with the mh-6.8.c package.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
November 24, 1999	**Ex-kcmx-configure86.c**	**Exploit script for Solaris 7 intel edition kcms_configure vulnerability, which gains root privileges**	
November 24, 1999	**Ie50.xml.txt**	**Exploit script for the Internet Explorer 5.0 XML HTTP redirect vulnerability.**	
November 24, 1999	Mdpag.c	Massively Distributed Penetration Attempt Generator, which generates fake scans on a target IP from a group of fake scanning IPs.	
November 24, 1999	**Nmap02.3BETA8.tgz**	**A utility for port scanning large networks.**	
November 24, 1999	NSS_252.tar.gz	Narrow Security Scanner is a perl script, which checks for 177 remote vulnerabilities.	
November 24, 1999	Smhijack.sh	Exploit script for the vulnerabilities in Sendmail 8.8.8 which hijacks incoming mail and saves it in /tmp.	
November 24, 1999	**Sol7.mailtool.txt**	**Solaris 7 script which exploits the mailtool, dtmail, and dtmailpr vulnerabilities.**	
November 24, 1999	WebCrack40.zip	A security tool that allows you to attempt to brute force ID and password combinations on your web site.	
November 24, 1999	**Wordpad.txt**	**Techniques on how to exploit the riched20.dll buffer overflow vulnerability.**	
November 24, 1999	Worldclient.2.0.0.0.dox.txt	Denial of Service exploit script for the buffer overflow vulnerability in WorldClient.	
November 22, 1999	Ifafoffuffoffaf.c	Integrated FTP attack facility. Remote exploit for wu-ftpd 2.5.0.	
November 22, 1999	**Rtfreadr.c**	**Exploit script for the WordPad buffer overflow vulnerability.**	
November 22, 1999	Shutup.c	Local Denial of Service exploit against syslog 1.3.	
November 22, 1999	**Xftpd.txt**	**Exploit for the Vermillion FTP daemon (VFTPD) Denial of Service vulnerability.**	
November 20, 1999	Knark-0.59.tar.gz	A kernel based rootkit for Linux 2.2	
November 19, 1999	Digital.voodoo.zip	Novice/intermediate hacking techniques and firewall penetration hacks.	
November 19, 1999	**Jetdirect.crash.txt**	**Technique for exploiting the JetDirect Denial of Service vulnerability.**	
November 19, 1999	NSS_251.tar.gz	A perl script, which checks for 177 remote vulnerabilities.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Comments
November 19, 1999	Pan_linux_b2.tgz	Pandora v4 Beta 2 for Linux BETA 2. Offline password auditing and online attack for the X Windows platform on Linux.	
November 19, 1999	Pan_online_95_b2.zip	Pandora v4 Beta 2 online for Windows 95/98 BETA 2. Online point and click attacking of Novell Netware from Windows 95/98.	
November 19, 1999	Pan_online_NT-b2.zip	Pandora v4 Beta 2 online for Windows NT BETA 2. Online point and click attacking of Novell Netware from Windows NT.	
November 19, 1999	Zetamail-2.1.txt	ZetaMail 2.1 POP3/SMTP Denial of Service exploit scripts.	
November 19, 1999	Zmaildox.exe	Binary for Windows and source for Windows ZetaMail vulnerability.	

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While this section will list only short descriptions, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

Trends for this two-week period:

- New variations of the Melissa virus continue to appear.
- Numerous systems are being root compromised via one of the most recent vulnerabilities in BIND.
- An increase in UDP scans on port 31789.
- An increase in ICMP Echo Reply Probes where no corresponding echo replies.
- **Numerous sites are being compromised via vulnerabilities in IIS web servers and MS Data Access Components (MDAC) vulnerabilities. (CyberNotes 99-22).** The Microsoft Data Access Components (MDAC), a part of Windows NT, and the RDS (Remote Data Services) DataFactory object vulnerabilities are currently the primary means for successful attacks on NT systems.
- An increase in widespread probes to port 98/tcp has been seen.
- We have received reports about intruders compromising machines in order to install distributed systems used for launching packet-flooding Denial of Service attacks. Two of the tools being used are trinoo and tribe flood network (or TFN). These tools appear to be undergoing active development, testing and deployment on the Internet.
- Two vulnerabilities are being used together to gain access to vulnerable systems. The first is rpc.statd, a program used to communicate state changes among NFS clients and servers. The second is in automountd, a program used to automatically mount certain types of file systems.

- Intrusion detection systems ranging from home computers with cable modems to high-end government facilities have been reporting a large number of probes to TCP ports 80, 8080 and 3128.
- Intruders are using distributed network sniffers to capture usernames and passwords. UDP packets containing username and password information may be sent to one or more remote sniffer servers using source port 21845/udp.
- Increased intruder activity has been noticed involving the am-utils package.
- An increase in widespread probes to port 21/tcp has been seen.

Viruses

W97M.Melissa.AA: The virus is a modified variant of the W97M.Melissa.A virus. The key changes made from the original W97M.Melissa.A virus are:

- the virus module name (now called "x");
- the e-mail subject/message;
- a malicious payload that deletes some text from the active document.

As its primary payload, the virus will attempt to use Microsoft Outlook to e-mail a copy of the infected document to as many as 100 people. When a user opens or closes an infected document, the virus first checks to see if it has done this e-mailing once before by checking the following registry key:

HKEY_CURRENT_USER\Software\MicrosoftOffice\

If this key has a value name "x" and value data "y", then the e-mailing has been done previously from the current machine. The virus will not attempt to do the mass mailing a second time from the current machine. If it does not find the registry entry, it will e-mail a payload similar to W97M.Melissa.A. The difference is that it mail itself to 100 addresses, and the subject line is:

Duhalde Presidente USERNAME

Where USERNAME is taken from the MS Word setting, and the e-mail message is:

Programa de gobierno 1999 – 2004.

The second payload is triggered when Day (Now) +1 = Minute (Now) +2.

W97M.Prilissa.A: This is another variant of the W97M.Melissa.A virus. It infects Word 97 documents and is spread by sending an infected document as an attachment to an e-mail message. When an infected document is opened, the virus disables virus protection security settings, conversion confirmation and recently opened file list. The first time the virus is executed on a system, it sends e-mails using Microsoft Outlook to the first 50 addresses in each of the address lists. The message contains "Message From (username)" in the subject line where (username) is the user name on the system. The body of the message contains:

"This document is very Important and you've GOT to read this!!!"

The infected document is sent as an attachment to the message. The virus modifies the Windows registry so that it does not send e-mail upon subsequent execution of the virus.

On December 25, several payloads are triggered. The virus displays the message box mentioned above. It also overlays several colored shapes onto the currently opened document. In addition, it overwrites the AUTOEXEC.BAT to format the C: drive and displays the following text upon the next reboot of the system:

Vine…Vide…Vice…Moslem Power Never End!!!
Your Computer Have Just Been Terminated By = CyberNET = Virus!!!

Then the virus copies itself to the global template in NORMAL.DOT. Once, NORMAL.DOT is infected, the virus infects documents when the file is closed from Word. It also disables the Tools/Macro menu so that the viral macros are hidden.

Some of the variable and function names in the viral code change upon replication. The virus keeps a list of labels in its code. Upon infection, the virus randomly changes each of the labels to another label in the list.

Worm.ExploreZip(pack): This is a packed version of Worm.ExploreZip, which contains a malicious payload. The worm utilizes MAPI-capable e-mail programs on Windows systems to propagate itself. The worm e-mails itself out as an attachment with the filename "zipped_files.exe". The body of the e-mail message may appear to come from a known e-mail correspondent and contains the following text:

I received your e-mail and I shall send you a replay ASAP.
Till then, take a look at the attached zipped docs.

Once the attachment is executed, it will unpack itself and execute the original Worm.ExploreZip routine. It may display an error message informing the user that the file is not a valid archive.

The worm proceeds to copy itself to the C:\WindowsSystem directory with the filename "Explore.exe" and then modifies the WIN.INI file so that the program is executed each time Windows is started. The worm then utilizes your e-mail client to harvest e-mail addresses in order to propagate itself. Users may notice that their e-mail client launches when this occurs.

W32.Mypics.Worm: This worm has several aliases including Worm.Mypics and Pics4you. It is received in an email attachment this the attachment called pics4you.exe. The subject line is blank and the body of the email is:
'Here's some pictures for you!'
This worm propagates on Windows 9x and Windows NT platforms.

When executed, the worm appears to have behavior similar to W97M/Melissa virus in that it distributes itself to 50 people in the address book. The user may notice that program appears to terminate, without displaying any pictures.

Once executed, the worm sets Microsoft Internet Explorer browser's "Home Page" to: http://www.geocities.com/SiliconValley/Vista/8279/index.html and a Windows registry keys will be modified to load the worm in memory every time the computer system is rebooted.

This worm has two payloads that simulate Y2K problems.

The first payload is executed when the worm detects the year 2000 (i.e. Jan 1, 2000). The worm executes a file named CBIOS.COM. This file modifies the system BIOS by overwrite the high byte of the two-byte CMOS checksum value in the system BIOS and insert a new autoexec.bat. As a result, on the next reboot the computer will display the message: "CMOS Checksum Invalid" and the computer will not boot. Entering the system BIOS setup utility and re-saving the BIOS data can correct the BIOS modifications.

If the BIOS settings are corrected, the new autoexec.bat file will execute. The new autoexec.bat file contains the following:
ctty nul format d: /autotest /q /u format c: /autotest /q /u
If rebooted, both the C and D drives will be reformatted.

This worm can be removed by ending the mypic process in the Windows Task Manager (processes tab). The user must also remove the following registry entry:

HKEY_LOCAL_MACHINE\Software\Microsoft\
Windows\CurrentVersion\Run= C:\Pics4You.Exe

HKEY_LOCAL_MACHINE\Software\Microsoft\
WindowsNT\Windows\Run= C:\Pics4You.Exe

Trojans

The following table provides the reader with a list of Trojans that have received write-ups in this publication. This table starts with Trojans discussed in CyberNotes #99-20 and will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks.

Trojan	Version	Issue discussed
Acid Battery	**1.0**	**Current Issue**
Ambush		**Current Issue**
Backdoor	0.1	CyberNotes 99-21
BioNet	**0.84-0.92**	**Current Issue**
Bla	1.0-2.0	CyberNotes 99-22
BladeRunner		CyberNotes 99-22
Bobo		CyberNotes 99-20
Bobo	**1.0-2.0**	**Current Issue**
BrainSpy	Beta	CyberNotes 99-21
Cain	**1.50-1.51**	**Current Issue**
Deepthroat	3.1	CyberNotes 99-20
Der Spacher	**3.0**	**Current Issue**
Doly	1.1-1.6	CyberNotes 99-20
Doly	**1.1-1.7**	**Current Issue**
Donald Dick	1.52	CyberNotes 99-20
Donald Dick	1.53	CyberNotes 99-22
Eclipse 2000		CyberNotes 99-20
Girlfriend	**1.3x (including patch 1)**	**Current Issue**
InCommand	1.0 (added 1.2)	CyberNotes 99-24
Ini Killer	2.0-3.0	CyberNotes 99-21
Irc3		CyberNotes 99-21
Logged		CyberNotes 99-21
Malicious		**Current Issue**
Matrix	1.4-1.5	CyberNotes 99-20
Matrix	**1.4-1.7**	**Current Issue**
Millennium	1.0-2.0	CyberNotes 99-21
Naebi	2.12-2.34	CyberNotes 99-22
NetSphere	1.0-1.31337	CyberNotes 99-20
NetSpy	1.0-2.0	CyberNotes 99-22
Phaze Zero	1.0b - 1.1	CyberNotes 99-23
Revenger	1.0	CyberNotes 99-23
RingZero		CyberNotes 99-22
Ripper		CyberNotes 99-22
SpiritBeta	1.2f	CyberNotes 99-22
SubSeven	1.0-2.0	CyberNotes 99-21
SubSeven	**1.0-2.1**	**Current Issue**
Thing	1.00 - 1.60	CyberNotes 99-23
Transmission Scout	1.1 - 1.2	CyberNotes 99-23
Vampire	1.0 - 1.2	CyberNotes 99-23
WarTrojan	1.0-2.0	CyberNotes 99-21
Xplorer	1.20	CyberNotes 99-21
Xtcp	2.0-2.1	CyberNotes 99-24
Y2K Countdown (Polyglot)		CyberNotes 99-20

AcidBattery (November 19, 1999): This Trojan mirrors Netbus' features, however it adds new commands which freeze/lockup your computer, grab passwords stored in the system and opens an FTP server to your harddrive.

Ambush (November 19, 1999): This just seems to be another basic Trojan, most useful for its file transfer features.

BioNet (November 19, 1999): Added versions 0.84, 0.87, and 0.92. The 0.8x versions of the Trojan are for Windows 95/98 only. However, the 0.9x (and above) have versions each for 95/98 and NT. The client-server protocol is the same, so an NT client can hack a 95/98 infected machine and a 95/98 client can hack an NT infected system just the same. File transfer, message boxes, screen and key capture, move mouse, and reboot/shutdown are a few of its commands. You usually notice that you are infected because you no longer can reboot or shutdown the computer (as the Trojan won't shutdown). It also makes it impossible to reboot to MSDOS mode to delete the Trojan.

Der Spaeher (November 19, 1999): the Trojan's client was in German, thus it was fairly hard to determine its features. It seems to have file transfer commands, and it could open Webpages in your browser.

Malicious (November 19, 1999): This Trojan, which in itself is not a Trojan, is very destructive. When the Trojan is run, it simply makes changes to the system registry that hides and disables most functions of your Windows system. However, the program itself does not load into memory, nor does it load on reboots, or even after its done editing the registry. When run, it carries out five main goals: hides the Shutdown option in the Start menu; hides the Find option in the Start menu; hides the Run option in the Start menu; disables regedit.ext; and hides all icons on your desktop.

Matrix (November 19, 1999): This is a Trojan based on the source code to the Girlfriend Trojan. Its main feature seems to be an FTP like file server, and the ability to update the Trojan exe on a victim's computer to a newer version with a one-button click.

Cain (November 26, 1999): This is a password grabbing Trojan. Cain is the client, while Abel is the Trojan server. Cain can connect to an infected system, get any and all passwords, and for those that are encrypted, it will try to brute force them, and can do this with the aid of a dictionary file. Even if your passwords are random letters and number, it will eventually decrypt then. If your passwords are found in a dictionary, it will decrypt them much faster.

Bobo (November 26, 1999): Another Trojan, which is basically a small subset of commands from BackOrifice, with the same interface as the BackOrifice GUI. This Trojan has no registry editor commands or plug in support.

Doly (November 26, 1999): Doly is a fairly damaging Trojan, which is also one of the most difficult to get rid of. Some of the features of this Trojan are:

- Trojan comes in setup.exe installer form pretending to be a memory manager;
- Single button "format harddisk" command;
- FTP server of harddrive;
- Can change "owner name" shown in System control panel;
- Change Window names, close, move, etc. windows;
- Change most monitor settings.

Version 1.2 adds an IP scanner and also a new feature, where the Trojan signs an invisible drone onto IRC where others in the same channel will see that you are infected and have your IP/host.

Girlfriend updated to include Patch 1 (December 2, 1999): Girlfriend in designed to let you steal information from the infected PC. Below is a list of some of its features:

- Text, that “infected” user enters to any window containing password field;
- Passwords, which “infected” user enters to password fields;
- Send “system” messages to remote PC;
- Play sounds;
- Show bitmaps (.bmp pictures);
- Send “victim” to any URL;
- Change server’s port’
- Hide GF Client with BOSSKEY=F12;
- Scan subnet for infected servers;
- Ping server;
- Save Windows list;
- Also takes passwords from websites, which infected user inputs.

SubSeven updated to include 2.1 (December 2, 1999): The SubSeven Trojan has the exact feature list as NetBus, with one original feature: The server can send the malicious user your IP when you connect to the Internet by either/any of e-mail, IRC, or ICQ.

New with version 2.1, the Trojan can be controlled not only via the SubSeven client, but also by messages sent to the IRC or ICQ drones the Trojan makes. This makes SubSeven very versatile and easy to use from a malicious user’s standpoint.